JUDGE BENJAMIN H. SETTLE

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. DONNIE BARNES, SR., Defendant.	No. 18-CR-5141 BHS MOTION TO SUPPRESS EVIDENCE **Noted: May 3, 2019**

I. INTRODUCTION

Donnie Barnes, Sr., through counsel, moves to suppress all fruits of summonses issued by the Department of Homeland Security (DHS) to Comcast, CenturyLink and Verizon, and all fruits of the search of his home on March 6, 2018, including all statements made by him in response to interrogation.

The summonses were issued on February 21 and March 12, 2018, by Homeland Security Investigations (HSI), a division of Immigration and Customs Enforcement (ICE), which is part of DHS. The summonses were served by HSI pursuant to 19 U.S.C. § 1509 and sought from each internet service provider (ISP) personal subscriber information associated with particular internet protocol (IP) addresses.

The summonses were illegal. Section 1509 strictly limits such summonses to customs enforcement matters and cannot be used to circumvent the need for subpoenas and warrants to obtain information in criminal cases.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Indeed, in November, 2017, the Office of Inspector General (OIG) for DHS issued a department-wide "Management Alert" to stop the misuse of summonses under § 1509 in criminal investigations. Exh. A. This followed earlier alerts within DHS regarding the improper use of §1509 summonses. Nevertheless, in this case, the Government ignored the law, its own policies and the requirements of the Fourth Amendment by unlawfully obtaining private subscriber information.

All fruits of that illegal conduct should be suppressed. The exclusionary rule is the only remedy for reckless or deliberate government abuse of a statutorily limited means of collecting personal information. Further, by continuing to use § 1509 summonses for criminal cases, in violation of the plain language of the statute and even after agents were directed not to use them, the Government's actions were unreasonable and it cannot claim good faith.

Mr. Barnes also seeks suppression of all evidence seized from his home, and the fruits of that evidence, because law enforcement executed a nighttime search of the home without good cause and in violation of the Fourth Amendment.

II. STATEMENT OF FACTS

Mr. Barnes is charged with one count each of production, distribution, and possession of child pornography.[1] On March 6, 2018, law enforcement executed a search warrant at his home. According to the supporting affidavit and other discovery, an Australian police officer saw a posting by user "TICK10T012TOCK" on a web site that allegedly served as a venue for illicit pictures. The posting included a photo that the affiant considered to be child pornography. The officer posted a comment and received an email from "dobsr@me.com," with the name "Donnie Barnes" associated with it.

[1] The production count is based on several pictures taken while the alleged victim was asleep. The issue of whether these images in fact constitute child pornography will be addressed separately if the Government's case survives the instant motion.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

The officer identified two IP addresses through which user "TICK10T012TOCK" had logged onto the site.

An HSI officer then issued summonses to CenturyLink, Verizon and Comcast for information related to the IP addresses. In response to the summons, Comcast disclosed that one of the IP addresses belong to an account in Spanaway and email user "dobsr@comcast.net." Further investigation, based on the information obtained from Comcast, led to a search warrant for Mr. Barnes's home at 100 174th Street in Spanaway. Exh. B (search warrant and supporting affidavit) at 12-13, ¶¶ 14-21. The Government would not have been able to obtain a search warrant without the information it had compelled from Comcast.

Before applying for a warrant, the affiant, HSI Special Agent Reese Berg, conducted surveillance outside Mr. Barnes's home on two dates, February 28 and March 1, 2018. On February 28, Agent Berg saw Mr. Barnes's partner leave the house at 6:30 a.m. with her two children. On March 1, Agent Berg saw Mr. Barnes leave the house at 6:02 a.m. Exh. B at 13, ¶¶ 22-25.

Finally, the warrant authorized execution of the warrant "at any time of the day or night." Exh. B at 33. The sole justification for that authorization was as follows:

> As part of this application, I am seeking authority to execute this warrant before 6:00 a.m. Given the observations of the SUBJECT PERSON's morning routine described above, I believe they may depart for work prior to or near 6:00 a.m. I would prefer to execute this warrant while all occupants of the SUBJECT PREMISES are present. To maximize the chances of that being the case, I hope to execute this warrant between 4:00 and 6:00 a.m.

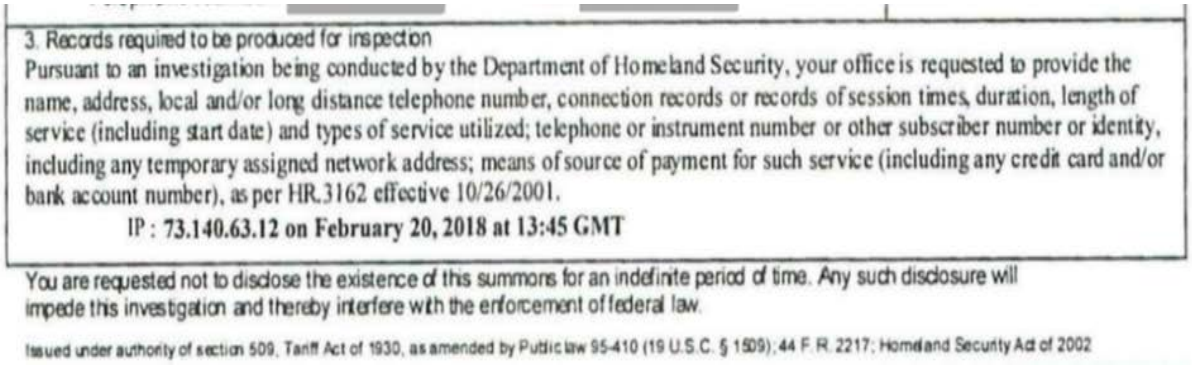
Exh. B at 14, ¶ 26.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

III. ARGUMENT

A. The Government Knowingly or Recklessly Violated the Law and the Fourth Amendment When it Demanded IP and Subscriber Information from Comcast and other ISPs.

The summons that DHS sent to Comcast and other ISPs stated that they were "required" to "produce" the following information:



3. Records required to be produced for inspection
Pursuant to an investigation being conducted by the Department of Homeland Security, your office is requested to provide the name, address, local and/or long distance telephone number, connection records or records of session times, duration, length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporary assigned network address; means of source of payment for such service (including any credit card and/or bank account number), as per HR.3162 effective 10/26/2001.

IP : 73.140.63.12 on February 20, 2018 at 13:45 GMT

You are requested not to disclose the existence of this summons for an indefinite period of time. Any such disclosure will impede this investigation and thereby interfere with the enforcement of federal law.

Issued under authority of section 509, Tariff Act of 1930, as amended by Public law 95-410 (19 U.S.C. § 1509); 44 F.R. 2217; Homeland Security Act of 2002

Exh. C (Comcast summons) at Bates 208.

The summons stated that it was issued "under authority" of 19 U.S.C. § 1509, and further stated that "[f]ailure to comply with this summons will render you liable to proceedings in U.S. District Court to enforce compliance with this summons as well as other sanctions." *Id.*; *see also id.* at Bates 209 (claiming that failure to comply with the summons could lead the court "to punish such failure as a contempt of court").

The summons also instructed the recipients that they should not disclose the existence of the summonses and that disclosure would "interfere with the enforcement of federal law." The summons then falsely stated that production was required "in connection with an investigation or inquiry to ascertain the correctness of entries, to determine the liability for duties, taxes, fines, penalties, or forfeitures, and/or to ensure compliance with the laws or regulations administered by CBP and ICE." *Id.* at Bates 208.

The summonses were plainly unlawful and suppression is required for several reasons. First, 19 U.S.C. § 1509 is part of the Tariff Act of 1930 and expressly limits

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

the use of a summons under the Act to instances where there is a United States Customs Service inquiry concerning tariffs or the importation of merchandise; it is not a legal means of collecting information as part of a criminal investigation.[2]

Second, the summonses demanded production of records that DHS is not authorized to obtain under § 1509. As the summons forms used in this case plainly state, consistent with the statute, its scope is limited to records and bookkeeping entries related to taxes, import duties and customs matters.

Finally, as discussed in detail below, DHS's unlawful use of the summonses is no mere technicality. To the contrary, this misuse of governmental power to compel the production of sensitive personal information implicates substantial privacy interests and violates the Fourth Amendment. And, to make matters worse, DHS has previously prohibited its agents from using summonses in criminal cases, yet they continue to ignore both the law and their own departmental procedures. Suppression is therefore required not only to vindicate Mr. Barnes's Fourth Amendment rights, but also to deter future misconduct by DHS agents.

1. A Customs Summons Under 19 U.S.C. § 1509 May Only Be Used for the Purpose of Customs Enforcement.

As plainly stated in the statute and clearly indicated on the summonses, § 1509 confers limited authority on the Customs Service to compel disclosure of records only in connection with "any investigation or inquiry conducted for the purpose of ascertaining the correctness of any entry, for determining the liability of any person for duty, fees and taxes due or duties, fees and taxes which may be due the United States, for determining liability for fines and penalties, or for insuring compliance with the laws of the United States administered by the United States Customs Service[.]" 19

[2] In 2002, the United States Customs Service became the Bureau of Customs and Border Protection and was placed under the Department of Homeland Security.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

U.S.C. § 1509(a); *see also, generally*, *Peters v. United States*, 853 F.2d 692, 696 (9th Cir. 1988) ("The authority of an administrative agency to issue subpoenas for investigatory purposes is created solely by statute") (citing 3 B. Mezines, J. Stein & J. Gruff, Administrative Law § 20.02 (1988)).[3]

The first three listed items plainly relate narrowly to imports, and the meaning of the fourth term is "cabin[ed]" by the first three. *See Yates v. United States*, 135 S. Ct. 1074, 1085 (2015) (applying "the principle of noscitur a sociis—a word is known by the company it keeps—to 'avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words, thus giving unintended breadth to the Acts of Congress'") (quoting *Gustafson v. Alloyd Co.*, 513 U.S. 561, 575 (1995)). The fourth item similarly limits the authority of using a summons under it to insuring compliance with "the laws of the United States administered by the United States Customs Service."

Thus, when Congress granted the power of an administrative summons to the Customs Service, it was careful to limit this potentially intrusive authority to the regulatory functions of collecting "duty, fees and taxes" and ensuring compliance with tariffs and similar matters. The statute does not permit, nor was it intended to permit, law enforcement agencies to avoid the more stringent requirements of subpoenas and search warrants in criminal investigations.

If there were any confusion on the part of DHS agents about the legality of using a summons in the way that occurred here, DHS's own Special Agent Internal Operating Procedures explicitly limit the use of summonses. The Procedures, issued on April 15, 2016, state that § 1509 authorizes "the examination of records to ensure compliance

[3] Case law and statutes use various terms to refer to what is referenced here as a "summons." Sometimes they are referred to as "administrative summons," "summons," and "third-party subpoena." For purpose of clarity, the term "summons" is used in this memorandum.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

with customs law"; a summons issued under the statute "cannot be used in drug-smuggling or export investigations," or in any matter unrelated to the "limited criteria" of customs enforcement; and a summons can only be used to obtain information specifically "related to Title 8 and Title 19 violations." Exh. A at 4. (Title 8 pertains to aliens and immigration offenses, and Title 19 is the Tariff Act of 1930. Neither relates to sex offenses).

Nevertheless, between January 2015 and May 2017, DHS agents misused § 1509 summonses to such an extent that DHS's Inspector General concluded that they had violated departmental policy (and the law) "at least 1 out of every 5 times" they had issued a summons. Exh. A at 4.

In May, 2017, the Executive Director of CBP's Investigative Operations Division tried to address this pervasive abuse of investigatory powers by circulating an email "clarifying the limited contexts in which Section 1509 Summonses may properly be used" and specifying that "the issuance of a 1509 summons requires probable cause to *believe* that the *records relate* to an importation of merchandise that is prohibited." *Id*. at 3 (emphasis in original).

Finally, in November, 2017 (just four months before the summonses issued in this case), DHS generated a "Management Alert" about the misuse of § 1509 summonses by its agents. Exh. A. This alert followed an internal investigation of an illegal attempt by DHS agents to uncover the subscriber information for a Twitter account critical of President Trump. DHS withdrew the Twitter summons the day after Twitter sought an injunction against having to comply with it.[4]

[4] *See, e.g.*, https://www.reuters.com/article/us-twitter-lawsuit/twitter-pulls-lawsuit-over-antitrump-account-says-summons-withdrawn-idUSKBN1792N9 (last accessed April 16, 2019). The complaint that prompted the DHS investigation and alert, *Twitter v. U.S. Dep't of Homeland Security et al*, Case 3:17-cv-01916, N.D. Ca. April 6, 2017, is available at: https://s3.amazonaws.com/big.assets.huffingtonpost.com/show_multidocs.pl.pdf

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

In short, there can be no credible dispute that the seizure of subscriber information in this case was unlawful and that DHS knew it was unlawful.

2. A Customs Summons Can Only Compel Production of Importation-Related Documents for Tariff Enforcement Purposes, not Subscriber Records for a Criminal Case.

Not only did DHS violate the law by using § 1509 summonses in a criminal case, the summonses compelled ISPs to produce personal information that DHS could not lawfully obtain with a summons. Pursuant to the statute, DHS can only compel the production of records that fall within a narrow category defined in 15 U.S.C. § 1509(d)(1)(A). In fact, that provision specifies just two types of records that can properly be obtained with a summons.

First, DHS may summons records that are "required to be kept under section 1508 of this title." Section 1508 requires importers to maintain various records relating to their merchandise. *See United States v. Frowein*, 727 F.2d 227, 233 (2d Cir. 1984) ("Section 1508 … imposes recordkeeping requirements on those who import or cause goods to be imported."). Plainly, the records DHS seized here have nothing to do with imports or merchandise.

Second, § 1509(d)(1)(A) allows the use of a summons for records "regarding which there is probable cause to believe that they pertain to merchandise the importation of which into the United States is prohibited." Here again, the statute is both clear and narrow, and the records seized in this case are entirely outside the scope of the statute.

3. The Government's Actions Violated the Fourth Amendment.

The "basic purpose of [the Fourth] Amendment … is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (citation omitted). "[W]arrantless searches are typically unreasonable where 'a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing."' *Id*. at 2221 (citation omitted). Thus, "[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Id*. (citation omitted).

In this case, DHS acted unreasonably under the Fourth Amendment because it violated the law and intentionally or recklessly abused its power to serve summonses; it used summonses to seize evidence of alleged criminal wrongdoing; and the Government's unlawful actions implicate significant privacy interests.

The Supreme Court's recent decision in *Carpenter* makes plain the constitutional ramifications of the Government's conduct in this case. In *Carpenter*, agents had served orders under the Stored Communications Act (SCA), 18 U.S.C. § 2703(d), on cell phone companies for historical cell-site location information (CSLI), and used that information to identify suspects in a string of robberies.[5] Unlike a § 1509 summons, which is unilaterally issued by agents without even a preliminary showing of reasonable cause, the SCA at least requires agents to obtain a court order based upon a showing of "reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." *Carpenter*, 138 S. Ct. at 2212.

Nevertheless, after first concluding that the Government's "acquisition of [] cell-site [locations] records was a search within the meaning of the Fourth Amendment," *id.* at 2220, the Court held that the Constitution requires a warrant supported by probable cause to collect CSLI. Regardless of the fact that CSLI (like ISP subscriber

[5] CLSI is automatically generated every time a cell phone connects to cell towers, which it does almost continuously to find and maintain the best signal, and wireless carrier companies routinely save this information for business purposes. 138 S. Ct. at 2212.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

information) is maintained by third parties for routine business purposes, the Court was particularly concerned about the privacy implications of allowing the Government to use CSLI to reconstruct a person's activities over an extended period of time, thereby "revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations." *Id*. at 2217 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (opinion of Justice Sotomayor)).

The ISP information at issue in this case implicates similar, if not greater, privacy interests. The seizure of ISP subscriber information allows unfettered access to a detailed picture of the private online activities of a person or household, as the Supreme Court of Canada has noted. *R. v. Spencer*, 2014 SCC 43, ¶¶ 32, 46 (2014).[6] Once an IP address is linked to a particular person, it can be used to reveal his or her web activities (as specific as the subscriber's edits to a particular Wikipedia page), file-sharing activities, and records in web server log files.[7]

ISP subscriber information can also be used to ascertain a user's Internet search terms and consumer habits.[8] An IP address combined with subscriber information can reveal sensitive and private information regarding an individual's political inclinations, health, religion, and sexuality. *id*.; Canadian Privacy Commissioner Report at 4-5 (note 7, *supra*); *State v. Reid*, 945 A.2d 26, 33 (N.J. 2008) (citing Daniel Solove,

---

[6] Available at: https://www.canlii.org/en/ca/scc/doc/2014/2014scc43/2014scc43.html (last accessed April 16, 2019).

[7] *What an IP Address Can Reveal About You: A Report Prepared by the Technology Analysis Branch of the Office of the Privacy Commissioner of Canada* (May 2013), at 4 ("Canadian Privacy Commissioner Report") available at: https://www.priv.gc.ca/media/1767/ip_201305_e.pdf (last accessed April 16, 2019).

[8] *Spencer*, 2014 SCC 43, ¶ 46 (citing N. Gleicher, *Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web*, 118 YALE L.J. 1945, 1948-49 (2009)).

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Reconstructing Electronic Surveillance Law, 72 Geo. Wash. L. Rev. 1264, 1287 (2004)) (noting that, with the combination of subscriber information and IP addresses, the Government "can track a person's internet usage" and "learn the names of stores at which a person shops, the political organizations a person finds interesting, a person's … fantasies, her health concerns, and so on").

Indeed, IP addresses and subscriber information may deserve even greater protection than CSLI, given the additional constitutional protections for free speech and association that are implicated by seizing such information. Internet usage is now integral to the exercise of First Amendment rights. *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017) ("While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace - the 'vast democratic forums of the Internet'") (citation omitted). And the right to speak and associate anonymously is a well-established component of the First Amendment. *See, e.g., Buckley v. American Constitutional Law Found.*, 525 U.S. 182, 200 (1999) (invalidating, on First Amendment grounds, a Colorado statute that required initiative petition circulators to wear identification badges). Indeed, "[a]nonymity is a shield from the tyranny of the majority.... It thus exemplifies the purpose behind the Bill of Rights...." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995) (citations omitted).

Given these core constitutional rights and protections, the Government's misuse of its investigatory powers in this case should not go unchecked. *See also Doe v. 2TheMart.com Inc.*, 140 F. Supp. 2d 1088, 1092 (W.D. Wash. 2001) (quashing subpoena to ISP for subscriber information because "[t]he right to speak anonymously was of fundamental importance to the establishment of our Constitution.").

Importantly, this Court need *not* decide whether a warrant is required to obtain subscriber information. Unlike *Carpenter*, where agents had followed the existing

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

statutory requirements for obtaining CSLI and served a proper (if ultimately unconstitutional) order, in this case the Government ignored the requirements of § 1509 and obtained information that it was never allowed to collect in the first place. In other words, this is an easy case, because the Government did not even bother to heed the limits imposed by Congress on the use of § 1509 summonses. And, with the Government having so plainly violated the law, suppression is not only appropriate but necessary to deter future violations.

4. Suppression is Not Only Appropriate but Necessary to Deter Continuing Governmental Misconduct.

Applying the exclusionary rule in this case is the only way to remedy and deter governmental misconduct. Despite the straightforward restrictions Congress placed on the use of § 1509 summonses, and DHS's own policies and alerts against using them for criminal investigations, DHS agents have routinely used the summonses to seize ISP information that they have no authority to obtain.

Section 1509 summonses were issued in at least 43 criminal cases between January 2015 and May 2017, representing approximately 20% of the total summonses issued during that time period. Exh. A at 4.

Among other examples of illegal summonses, DHS used them improperly to obtain records from Craigslist in a matter involving a Border Patrol agent who allegedly attempted to sell government-issued night vision goggle, and even in cases where a CBP employee requested sick leave under false pretenses. *Id.* Incredibly, HSI agents also used a customs summons to seek information about Twitter accounts that criticized

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

a local prosecutor in Buenos Aires.[9] This summons was withdrawn only after it came to the attention of the Argentine press.[10]

Counsel is personally aware of other § 1509 summonses that DHS has recently issued to obtain ISP information. *See United States v. Edmond Smith*, CR17-207-JCC. Counsel has also been informed by Federal Defenders in other districts that DHS continues to use § 1509 summonses in criminal cases.

Given these facts, suppression is not only the appropriate remedy for the Government's unlawful actions, but a necessary deterrent to prevent continuing abuse of its investigatory powers. One of the exclusionary rule's main purposes "is to deter future unlawful police conduct[.]" *United States v. Calandra*, 414 U.S. 338 (1974). In particular, "the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Herring v. United States*, 555 U.S. 135, 144 (2009).

Deterring unlawful use of administrative summons powers is particularly important because that power can be so easily and widely abused. As the Third Circuit explained in *United States v. Genser*, 582 F.2d 292 (3rd Cir. 1978), suppression was the only practical remedy to curtail the misuse of administrative summonses under 26 U.S.C. § 7602 in criminal cases. That statute permitted the IRS to compel testimony and obtain documents only for the limited purpose of ascertaining the correctness of tax returns or to collect revenue. *Id.* at 308.

In another case where the IRS abused its statutory authority, the district court dismissed the criminal prosecution *sua sponte*, with prejudice, because it found the IRS

---

[9] Musgrave, Shawn and Sarah Jeong, *How ICE Used an Obscure Rule to Pursue the Owners of a Korean Porn Site*, The Verge, Sept. 27, 2018, available at" https://www.theverge.com/2018/9/27/15186356/ice-korean-porn-customs-law-soranet-spycam-homeland-security (last accessed April 16, 2019).

[10] *Id.*

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

had acted with institutional bad faith in gathering evidence for the prosecution. *United States v. Weiss*, 566 F. Supp. 1452 (C.D. Cal. 1983). The court concluded that "[a]ny such criminal use of Civil Summonses is not to be condoned or tolerated by the Judiciary." *Id.* at 1455.

Similarly, in *United States v. Dahlstrum*, 493 F. Supp. 966, 975 (C.D. Cal. 1980), the court felt "compelled" to dismiss an indictment with prejudice when there was "overwhelming evidence" of a federal agency "flouting the civil summons authority granted to it by Congress," even though it was "fueled only by 'institutional bad faith' and not any personal bad faith."

Here, DHS has itself acknowledged persistent abuse of its civil summons authority and its sporadic internal efforts to end the abuse have failed. The necessary recourse in this case, short of dismissal with prejudice, is the exclusionary rule both to vindicate Mr. Barnes's constitutional rights and to ensure that DHS's abuse of its summons authority comes to a long overdue end.

B. The Fruits of the Search Warrant Should Be Suppressed Because The Nighttime Execution of the Warrant Violated The Fourth Amendment.

A judge issuing a search warrant must "command the officer to . . . execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time[.]" Fed. R. Crim. P. 41(e)(2)(A)(ii). "Daytime" is defined as between 6 a.m. and 10 p.m. Fed. R. Crim. P. 41(a)(2)(B).

In this case, the warrant was executed at 5:15 a.m. on March 6, 2018, one hour and 24 minutes before sunrise.[11] The judge who issued the warrant authorized its execution "at any time in the day or night," *see* exh. B, but there was no good cause for doing so. To the contrary, the affiant merely stated in the warrant application that he

[11] *See* timeanddate.com, reporting that sunrise in Spanaway on March 6, 2018 was at 6:39 a.m.: https://www.timeanddate.com/sun/@5811581?month=3&year=2018

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

"would prefer to execute this warrant while all occupants of the SUBJECT PREMISES are present," and to "maximize the chances" of that occurring, he "hope[d]" to execute the warrant between 4 a.m. and 6 a.m. *See* exh. B at ¶ 26.

Whatever the agent's "preference" might have been, he offers no basis for concluding that a nighttime search was necessary. To the contrary, this was a routine internet-related investigation. The warrant application itself states that the evidence sought is typically retained by suspects "for many years" and can be recovered with forensic tools even after it has been deleted. Exh. B at Bates 21, ¶ 45 (even when digital evidence is intentionally deleted, it "can often be recovered, months or even years later" using forensic tools). And there is nothing to suggest that Mr. Barnes was dangerous or otherwise any different from other suspects in pornography cases in which warrants are routinely executed during normal daytime hours. Indeed, in all his years of criminal practice, this is the first time that defense counsel has seen or heard of a nighttime residential search in this type of case.

There is little law addressing good cause for nighttime searches, perhaps because in the relatively infrequent instances in which authority for such searches has been granted the need is well-supported by the warrant application. Hence, in *United States v. Kelley*, 652 F.3d 915, 917 (8th Cir. 2011), the court noted that the constitutional question of nighttime searches had received "surprisingly little attention[.]" There, the court did not suppress because the warrant had authorized execution at any time based on the affidavit demonstrating that "the objects to be seized are in danger of imminent removal." *Id.* at 916. Here, the opposite is true, since the affidavit showed that the evidence sought was highly unlikely to disappear.

Similarly, in *United States v. Gibbons*, 607 F.2d 1320, 1326 (10th Cir. 1979), the court stated, "The Amendment itself spoke in terms of protection 'against unreasonable

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

searches and seizures' and it seems logical that the factor of a nighttime search is sensitively related to the reasonableness issue."

In discussing the concerns animating the adoption of the Fourth Amendment, the *Gibbons* court emphasized Justice Frankfurter's observation that "[s]earches of the dwelling house were the special object of this universal condemnation of official intrusion. Night-time search was the evil in its most obnoxious form." 607 F.2d at 1326, quoting *Monroe v. Pape*, 365 U.S. 167, 210 (1960), *overruled on other grounds*, *Monell v. Dep't of Soc. Servs. of N.Y.*, 436 U.S. 658 (1978) (Frankfurter, J. concurring and dissenting) (footnote omitted). As in *Kelley*, the *Gibbons* court did not suppress, in this case because the search was of a car trunk, thus not implicating the concern about intrusions into a home, and because the affidavit demonstrated "the necessity of immediate police action[.]" *Id.* at 1327; *see also O'Rourke v. City of Norman*, 875 F.2d 1465, 1473-75 (10th Cir. 1989) (§ 1983 action in which the court concluded that nighttime execution of a warrant violated the Fourth Amendment). Here, by contrast, the police raided Mr. Barnes's home, and there was no claim that immediate action was needed.

Counsel is unaware of any Ninth Circuit authority explicitly addressing the constitutionality of nighttime searches absent "good cause." However, the decision in *Bravo v. City of Santa Maria*, 665 F.3d 1076 (9th Cir. 2011), gives a strong indication of the Ninth Circuit's view. In that case, the plaintiff alleged Fourth Amendment violations and the court reversed the lower court's ruling that omissions from an affidavit were not material and were neither intentional nor reckless. What is instructive is the court's discussion after reaching that conclusion.

In *Bravo*, Javier Bravo, Jr. was involved in a shooting and the police executed a search warrant before sunrise at the home where he lived with his parents. However, Bravo was in custody at the time of the search, a fact that was not disclosed in the

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

warrant application. The Ninth Circuit stated, "once the affidavit was corrected and supplemented with the missing information about Javier Jr.'s custody status, even if we were to conclude that cause existed for a search, there would still be no basis for authorizing nighttime service." *Id.* at 1085. The court subsequently observed, "Had Javier Jr.'s incarceration been disclosed and probable cause for a search still existed, no reasonable cause for nighttime service would have remained under the totality of the circumstances." *Id.* The court further concluded that, with the omitted information included, "it is extremely doubtful that an issuing judge would simply have issued the warrant or authorized nighttime service without more information." *Id.*

Gibbons and *Kelley* are correct, and they are reinforced by the discussion of nighttime searches in *Bravo*; absent a clear showing of a particularized need for a nighttime search, it is unreasonable under the Fourth Amendment to execute a warrant at night. *Cf.* Wayne LaFave, 2 Search & Seizure § 4.7(b) (5th ed.) ("it is submitted that the true test of the constitutionality of a nighttime search is *whether it was necessary to make the search at that time*") (emphasis added).

Given the facts in this case, in which there is not even a pretense of good cause for a nighttime search, suppression is the appropriate remedy. The Government is also precluded from relying on the good faith doctrine to escape the consequences of this violation. "[T]he good-faith exception is not relevant where the violation lies in the *execution* of the warrant, not the validity of the warrant." *United States v. Gantt*, 194 F.3d 987, 1006 (9th Cir.1999), *reversed on other grounds, United States v. W.R. Grace*, 526 F.3d 499 (9th Cir. 2008) (emphasis in *Gantt*). Even if the good faith doctrine were applicable, the grounds provided in the affidavit were so patently insufficient that no reasonable officer could have relied on the authorization, thus bringing this warrant within the "bare bones" exception to the good faith doctrine. *See United States v. Leon*, 468 U.S. 897, 915 (1984).

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

IV. CONCLUSION

The Court should suppress all fruits of the DHS summonses and resulting search warrant, including any statements by Mr. Barnes.

DATED this 22nd day of April, 2019.

Respectfully submitted,

s/ Colin Fieman
Attorney for Donnie Barnes, Sr.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

CERTIFICATE OF SERVICE

I hereby certify that on April 22, 2019, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notification of filing to all registered parties.

s/ *Carolynn Cohn*
Paralegal

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710